Subject : 2170709-Information and Network Security

Prof. Rupesh G Vaishanv

Sr.	Unit No.	Question
1	1	Explain Playfair Cipher in detail. Find out cipher text for the following given plain text and key. 1. Key = GOVERNMENT Plain text = PLAYFAIR 2. Plain Text= “INFORMATION AND NETWORK SECURITY”, Key = “MONARCHY” 3. Key=“hidden” , Plain Text= “Message” 4. Plain Text= “Surgical Strike” key = “GUJAR” 5. Key = ENGINEERING Plaintext=COMPUTER
2	1	Encrypt the message using the Hill cipher algorithm 1. Plain Text= “GTU Examination” key matrix = 5,17|4,15 2. Key K=17,17,17|21,18,21|2,2,19 Plaintext =”ney” 3. Plain Text= "meet me at the usual place " Key = 9,4 | 5,7
3	1	Describe Rail-fence cipher algorithm with example. Or Explain columnar transposition Cipher technique.
4	1	Explain cryptanalytic attacks with example of any encryption algorithm. Or Discuss the following terms in brief: - Passive attack - Cryptanalysis Or Briefly explain any two active security attacks.
5	1	Define terms Confidentiality, Integrity, Availability, Authentication, Authorization, Non –repudiation
6	2	Explain AES encryption in detail. Or Explain four different stages of AES(Advance Encryption standard) structure. Or Briefly describe Mix Columns and Add Round Key in AES algorithm.
7	3	Discuss any two of the following block cipher modes of operation in detail with neat sketches 1. Electronic Code Book (ECB) 2. Cipher Block Chaining (CBC) 3. Cipher Feedback (CFB) 4. Output Feedback (OFB) 5. Counter (CTR)
8	4	Explain process of encryption in RSA Algorithm with suitable example. (Prime Number P,Q and Encryption Key E is given for reference) P=7, Q=17, E=7 Or In a public key cryptosystem using RSA algorithm, user uses two prime numbers 5 and 7. He chooses 11 as Encryption key , find out decryption key. What will be the ciphertext, if the plaintext is 2? Or Explain in detail RSA algorithm, highlighting its security aspect. Or P and Q are two prime numbers. P=7, and Q=17. Take public key E=5. If plain text value is 6, then what will be cipher text value according to RSA algorithm? Explain in detail.
9	4	Briefly explain Diffie Hellman Key exchange with an example Or Calculate the shared secret (KA and KB) key using Diffie Hellman Key Exchange Algorithm. Take q=23, α = 5, XA = 6 and XB = 15. Or For Diffie-Hellman algorithm, two publicaly known numbers are prime number 353 and primitive root of it is 3. A selects the random integer 97 and B selects 233. Compute the public key of A and B. Also compute common secret key.

* Given marks are based on previous GTU Papers

10	5	Explain working of Secure Hash Algorithm, with basic arithmetical and logical functions used in SHA. Or Write a detailed note on Secure Hash Algorithm.
11	5	Discuss HASH function and its application in Crypto System. Or Explain basic Hash code generation. Or What is the role of a compression function in a hash function?
12	6	Write a note on: Message Authentication Codes Or What is MAC ? How it useful in Crypto System.
13	7	Explain digital signature schemes Elgamal and Schnorr.
14	7	Write a short note on “Digital Signature Algorithm”. Or What is the principle of digital signature algorithm(DSA). How a user can create a signature using DSA? Explain the signing and verifying function in DSA.
15	8	Explain use of Public-Key Certificate with diagram and draw X.509 certificate format.
16	8	Explain various general categories of schemes for the distribution of public keys. Or Explain various public key distribution techniques. Or What is KDC? List the duties of a KDC.
17	8	Write a short note on public key infrastructure.
18	9	Write a detailed note on: Kerberos. Or Explain authentication mechanism of Kerberos.
19	10	Write a short note on SSL. Or Explain HAND SHAKE protocol in SSL. Or Briefly discuss the working of SSL Record Protocol.
20	10	Explain HTTPS and SSH.

* Given marks are based on previous GTU Papers